

MELINDA HAAG (CABN 132612)
United States Attorney

MIRANDA KANE (CABN 150630)
Chief, Criminal Division

DAVID R. CALLAWAY (CASBN 121782)
Assistant United States Attorney

150 Almaden Avenue, Suite 900
San Jose, California 95113
Telephone: (408) 535-5596
Facsimile: (408) 535-5066
E-mail: David.Callaway@usdoj.gov

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE FEDERAL CRIMINAL
INVESTIGATION

No. CR 13-70550 HRL

ORDER DIRECTING THE CLERK OF
COURT TO MAINTAIN ORIGINALLY-
FILED COMPLAINT UNDER SEAL AND
TO FILE SUBSTITUTE VERSION
[proposed]

Based on the request made by Plaintiff United States of America in open court on May 16, 2013, with the concurrence of the defendant, and for good cause shown,

IT IS HEREBY ORDERED as follows:

(1) the captioned Criminal Complaint and supporting affidavit shall remain Under Seal, per this Court's order dated May 16, 2013 (signed May 15, 2013);

(2) the Clerk of Court shall file the attached version of said Criminal Complaint, in which certain names and other statements have been redacted to protect the privacy of witnesses and the minor victim, and make the attached version only available for inspection by the public;

(3) the Clerk of Court, in its discretion, may elect whether this is best accomplished

ORDER

Filed

MAY 17 2013

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

1 through the assignment of a new case number to the attached Criminal Complaint.

2 (4) this Order SUPERSEDES a similar order, dated May 16, 2013, directing the Clerk of
3 Court to file another redacted version of the Criminal Complaint and Supporting Affidavit. The
4 only version of the captioned Criminal Complaint and supporting affidavit that should be
5 available to the public is the version attached to this Order.

6 DATED:

5/17/13

7
8 
9 HOWARD R. LLOYD
United States Magistrate Judge
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

SEALED BY ORDER
OF THE COURT

OA 91 Criminal Complaint

United States District Court

NORTHERN

DISTRICT OF

Filed

MAY 16 2013

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

UNITED STATES OF AMERICA
V.
DAVID JOHN STEVENS

CRIMINAL COMPLAINT

13-70550

HRL

Case Number:

(Name and Address of Defendant)

I, the undersigned complainant being duly sworn state that the following is true and correct to the best of my knowledge and belief. On or about 4/14/2013 to 5/3/2013 in Monterey County, in the Northern District of California defendant(s) did,

(Track Statutory Language of Offense)

COUNT ONE: employ, use, persuade, induce, and coerce a minor, to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct, in and affecting interstate commerce, in violation of 18 U.S.C. 2251(a); and COUNT TWO: knowingly distribute a visual depiction using any means of interstate and foreign commerce, by any means including by computer, where that visual depiction involved the use of a minor engaging in sexually explicit conduct and depicted such conduct,

in violation of Title 18 United States Code, Section(s) 2252(a)(2)

I further state that I am a(n) Special Agent, HSI and that this complaint is based on the following facts:

SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT SCOTT BEAGLE, including Exhibit 1 thereto

MAXIMUM PENALTIES (Count One): not less than 15 nor more than 30 years imprisonment, \$250,000 fine; 5 year TSR; \$100 SAF

REQUESTED PROCESS: Arrest Warrant

REQUESTED BAIL: No Bail (government will request detention)

Continued on the attached sheet and made a part hereof:

☒ Yes ☐ No

Approved

As To

Form: DAVID R. CALLAWAY

AUSA

SCOTT BEAGLE

Name/Signature of Complainant

Sworn to before me and subscribed in my presence,

Date

5/15/13

at

SAN JOSE

CALIFORNIA

City and State

HON. HOWARD R. LLOYD

United States Magistrate Judge

Name & Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH AND ARREST WARRANT

I, Scott Beagle, a Special Agent with the San Jose Office of the Department of Homeland Security, Immigration and Customs Enforcement (ICE), being duly sworn, depose and state as follows:

I. INTRODUCTION AND PURPOSE FOR THE WARRANT

1. I submit this affidavit in support of a search warrant for 10 E. Bernal Drive, #3, Salinas, California (the "SUBJECT PREMISES"), as further described in Attachment A, and for the arrest of the defendant, David John STEVENS (STEVENS), who is further described as a white male adult, born on July 22, 1954, assigned California Driver's License number B3719544, and who resides at the SUBJECT PREMISES.

2. This affidavit pertains to an investigation into the possession, manufacture, and distribution of material involving the sexual exploitation of minors. Specifically, my office is investigating STEVENS's use of a computer at the SUBJECT PREMISES to create and distribute child pornography images [REDACTED]

[REDACTED] I respectfully submit that the facts set forth in this affidavit establish probable cause to believe that STEVENS has violated 18 U.S.C. §§ 2251 and 22522, which prohibit certain activities relating to material involving the sexual exploitation of minors, originating from the SUBJECT PREMISES, and that evidence, contraband, fruits, and instrumentalities of those crimes will be found within those SUBJECT PREMISES.

3. I request authority to search the entire premises, including the residential dwelling, and a vehicle, for the items specified in Attachment B, although any computers, computer media, external data storage devices, smart-phones, digital media players, and personal digital assistants (PDAs) will be seized rather than searched, as described more fully herein.

II. AGENT BACKGROUND

4. I am a Special Agent (SA) with the United States Department of Homeland Security (DHS), Homeland Security Investigations (HSI), presently assigned to HSI San Jose, California. I have been an HSI Special Agent (SA) since February 2010. Prior to my employment with HSI, I was employed as a Border Patrol Agent for approximately seven years. As a Special Agent with HSI, I am authorized to investigate violations of laws of the United States, and I am a law enforcement officer with authority to execute arrest and search warrants under the authority of the United States. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations of 18 USC 2252, 2242 and 2241. I am authorized to investigate computer crimes and crimes against children and have received training pursuant to both of those types of investigations, to include training related to the identification of images of child pornography, online Internet undercover investigations, and the recognition of known child victims within those images. I also received

specialized training in the area of child sexual exploitation. I have also been involved with approximately twenty (20) cases involving child exploitation. I have completed twenty weeks of training at the Federal Law Enforcement Training Center in Glynco, Georgia, including the Criminal Investigator Training Program. I have a Bachelor of Science degree in Criminal Justice from Wayland Baptist University.

5. The statements in this affidavit are based in part on information provided by HSI Special Agents as well as foreign law enforcement officials. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that STEVENS committed the violations described in this affidavit, and that evidence, fruits, and instrumentalities of those violations will be found at the SUBJECT PREMISES.

III. RELEVANT STATUTES

6. This investigation concerns alleged violations of 18 U.S.C. § 2252, relating to material involving the sexual exploitation of minors.

a. 18 U.S.C. § 2251(a) prohibits using, persuading, inducing, or coercing a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct, if the perpetrator knows or has reason to know that such visual depiction will be transmitted in or affecting interstate or foreign commerce.

b. 18 U.S.C. § 2252(a)(1) prohibits knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct.

c. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed, shipped, or transported in interstate or foreign commerce. That section also prohibits knowingly reproducing any visual depiction of minors engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail.

d. 18 U.S.C. § 2252(a)(4) prohibits possessing one or more matters containing visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce, or that were produced using materials that had traveled in interstate or foreign commerce.

IV. DEFINITIONS

7. The following definitions apply to this Affidavit and the attachments thereto:

a. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

b. "Storage Medium" is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and DVDs.

c. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (such as central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, disk drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

d. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to unlock or decode particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

e. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

f. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

h. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

i. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C), engaged in actual or simulated (a) sexual intercourse (whether genital-genital, oral-genital, or oral-anal) between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

j. "Visual depictions" include undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. 18 U.S.C. § 2256(5).

k. The terms "records," "documents," and "materials" include information recorded in any form, visual or aural, and by any means, whether by hand, photograph, video, or photocopy, by analog recording, printing, or typing, or by digital recording, transmission, or storage in any format and on any analog or digital storage device, including tape recordings, cassettes, compact discs, hard disks, CD-ROMs, DVDs, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, smart phones such as iPhones or Blackberrys, media players such as iPods, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device.

V. FACTS SUPPORTING PROBABLE CAUSE

8. As set forth in Exhibit 1, a referral from the Danish National Police resulted in the issuance of an arrest warrant for a person identified only as "John DOE." The arrest warrant was signed on May 10, 2013, by The Honorable Alan Kay, United States Magistrate Judge for the District of Columbia, Case 1:13-mj-361. John DOE was described only as a "white male, 45-55 years old, heavy-set build, balding with wreath of light brown hair, brown mustache." The facts set forth in Exhibit 1, which describe four sexually-explicit videos involving John DOE and a then-unidentified minor female, are incorporated fully here by reference. The following facts describe how we came to identify John DOE as the defendant, STEVENS, and his residence as the SUBJECT PREMISES.

9. On May 15, 2013, Homeland Security Investigations (HSI) Special Agents Stebbins and Roche interviewed [REDACTED]. The day before, [REDACTED] had contacted the HSI Tip Line after identifying [REDACTED] as being sought by law enforcement in a child pornography investigation. [REDACTED] told the agents that on May 14, 2013, she was viewing her Facebook account where she saw a posting for the NCMEC (National Center for Missing and Exploited Children) website. On the NCMEC website, [REDACTED] recognized [REDACTED] STEVENS, from

the posted pictures— [REDACTED]
[REDACTED]

10. SA Stebbins asked [REDACTED] how she was able to identify [REDACTED] in the photographs. [REDACTED]

[REDACTED] NCMEC obtained the photographs from HSI's Cyber Crime Center (C3) where snapshots of videos were taken. The videos, which are more particularly described in Exhibit 1, depicted child pornography where an adult male was sexually violating a prepubescent female. The C3 produced snapshots of an adult male, the prepubescent victim, and the room where the abuse was videotaped, in order to publicize them in an effort to identify the perpetrator.

11. From those still photographs, [REDACTED] identified the shoes and watch STEVENS was wearing. [REDACTED] also identified an all-in-one printer, scanner, fax machine, a music chair, the blue carpet within the room, and a white trash can used for recycling. All these items were located within the screen shot that C3 had provided to NCMEC. [REDACTED] the photograph was taken inside a private sound-proof room located in the garage of [REDACTED] the SUBJECT PREMISES. [REDACTED]

[REDACTED] Stevens had several computers in the music room as well as a web camera affixed to the wall. [REDACTED]
[REDACTED]

12. [REDACTED]
[REDACTED] described [the victim] as being 11 years old, [REDACTED]
[REDACTED] identified sanitized pictures of the child sexual abuse victim depicted in the C3/NCMEC photographs [REDACTED]

13. On that same date, SAs Stebbins and Roche [REDACTED]
[REDACTED] who advised that [REDACTED]
[REDACTED] in October 2012, he had confronted STEVENS on one occasion [REDACTED]
[REDACTED]

14. SA Stebbins also showed the sanitized pictures of the child sexual abuse victim depicted in the C3/NCMEC videos. [REDACTED] positively identified [REDACTED] the victim depicted in those photographs.

15. SA Stebbins has also obtained a California Driver license photo of

STEVENS. He, too, believes that the person depicted in the C3 screenshots is STEVENS.

VI. BEHAVIORAL CHARACTERISTICS OF CHILD PORNOGRAPHY OFFENDERS

16. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and who receive or distribute images of child pornography, including:

- a. Persons who have a sexual interest in children and who manufacture, possess, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have while viewing children engaged in sexual activity or in sexually suggestive poses, whether in person, in photographs, or on other visual media, or from reading descriptions of such activity.
- b. Persons who have a sexual interest in children and who receive or distribute child pornography may collect sexually explicit or suggestive depictions of children in a variety of media, including photographic prints, slides or negatives, magazines, videotapes, books, illustrations or computer printouts on paper, or digital media. These individuals often use these materials for their own sexual arousal and gratification. They may also use these materials to lower the inhibitions of children whom they are attempting to seduce, to arouse a selected child partner, or to demonstrate desired sexual acts.
- c. Persons who have a sexual interest in children and who receive or distribute child pornography often keep child pornographic material that is not stored in digital form in the privacy and security of their home or in an adjacent storage area, such as a garage or shed. They value this material and will typically retain it for many years.
- d. Likewise, persons who have a sexual interest in children and receive or distribute child pornography often maintain child pornographic material that is in a digital or electronic format in a safe, secure, and private environment, such as on a computer or on nearby storage devices and media. They value these collections and often maintain them for several years in an accessible place, usually at the collector's residence, so that they can view them at will.
- e. Persons who have a sexual interest in children and who receive or distribute child pornography also may correspond with and/or meet with others to share information and materials. They rarely destroy correspondence from other child pornography enthusiasts, they protect and conceal this correspondence as they do their sexually explicit material, and they often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share their interest in child pornography.

f. Persons who have a sexual interest in children and who receive or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.

VII. USE OF COMPUTERS, DIGITAL CAMERAS, AND THE INTERNET

17. Computers and digital technology have revolutionized the way in which individuals interested in child pornography interact with each other. Pre-digital age child pornography was produced using still, movie, or video cameras and film. To avoid detection, child pornography producers required darkroom facilities and a significant amount of skill to develop and print the images. Producing and distributing child pornography was relatively expensive and time-consuming. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public.

18. Computers and digital technology have changed the production, distribution, and storage of child pornography, and the communication among child pornography producers, distributors, and consumers.

19. *Production.* Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 4 gigabytes of data, which provides enough space to store over 1000 high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

20. *Communication and Distribution.* A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

21. *Storage.* The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years; 500 gigabyte external and internal hard

drives are not uncommon. These drives can store thousands of images at very high resolution. In addition, child pornography can be easily stored on CDs, DVDs, thumb drives, digital memory cards, and portable digital music and video players such as iPods, which can double as high-capacity storage media, personal digital assistants such as Palm PDAs, or multimedia "smart phones" such as iPhones, Palm Treos, or Blackberrys, all of which can store digital media. All of these media are easy to use.

22. The Internet allows individuals to obtain, view, and trade child pornography in a relatively secure and anonymous fashion. The Internet offers online resources to retrieve and store information that can be easily and cheaply used to store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail. These online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can usually be found on the user's computer or external media.

23. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or by saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, when, for example, traces of the path of an electronic communication are automatically stored in cache files. A computer user's Internet activities generally also leave traces or "footprints" in the web cache and history files of the browser used. The computer often maintains this information indefinitely until it is overwritten by other data.

VIII. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

24. As described above and in Attachment B, this application seeks permission to search and seize non-digital records that might be found within the SUBJECT PREMISES, but only to seize computers and other digital media. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that records can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes, memory chips and other storage media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

25. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the

file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

26. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

27. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

28. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

29. Based on my training and experience, I believe that computers and computer storage media at the SUBJECT PREMISES will not only contain direct evidence of the crimes described on the warrant, but also evidence that establishes how the computers were used, the purpose of their use, who used them, and when.

30. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), computer storage media can contain other forms of electronic evidence as well:

a. Data on a digital storage medium that is not currently associated with any file can provide evidence of a file that was once on the storage medium but that has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user

attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance with particularity a description of the records to be sought, evidence of this type often is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish the absence of particular data on a storage medium.

31. Based upon my knowledge, training and experience, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. A child pornography collector may not organize contraband in a fashion immediately recognizable to a forensic analyst. Sorting contraband and evidence of crime from innocuous digital data could take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

c. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge

that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

32. Because several people may share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on any of those computers or storage media, this application seeks permission to seize those computers or storage media as well. It may be impossible to determine, on scene, which computers or storage media contain the things described in this warrant.

IX. SEIZURE OF FORFEITABLE PROPERTY

33. This application requests the issuance of a warrant under 18 U.S.C. § 2253, and by reference 21 U.S.C. § 853(f), authorizing the seizure of property subject to forfeiture. This is appropriate because: (1) there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture, and (2) an order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture. There is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture, because 18 U.S.C. § 2253 provides that the defendant's interest in any personal or real property that was used or intended to be used to commit or to promote the commission of such offense shall be forfeited to the United States.

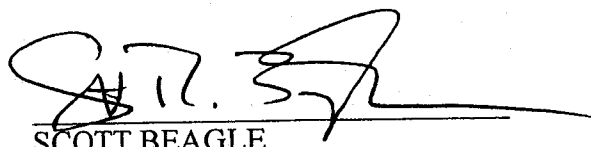
X. CONCLUSION AND SEALING REQUEST

34. I believe the facts set forth in this affidavit constitute probable cause both that STEVENS has violated 18 U.S.C. §§ 2251 and 2252, and that evidence of those violations, as more fully described in Attachment B, will be found at the SUBJECT PREMISES. Therefore, I respectfully request issuance of the warrant for STEVENS's arrest and the attached search warrant for the SUBJECT PREMISES. I believe that an arrest warrant issued by this Court, now that we have identified the former "John DOE" as STEVENS, a person residing in this district who committed the foregoing offenses here, should supplant the "John DOE" arrest warrant attached as Exhibit 1.

35. This search warrant relates to an ongoing federal investigation into the manufacture, distribution, and receipt of child pornography, and I believe that disclosure of the facts of this investigation may alert potential targets, subjects, and witnesses to the investigation, resulting in their flight or the destruction or concealment of evidence, and may compromise ongoing related investigations. (STEVENS is himself under arrest, but

there may be other confederates we do not know about.) Accordingly, I request that the Court issue an order sealing the search warrant, this affidavit, the application and all exhibits and attachments thereto, and the sealing application and order itself, until further order of this Court.

36. Attachments A, B, and C are incorporated fully here by reference. When he was arrested on the afternoon of May 15, 2013, STEVENS acknowledged that the gray Chevy Tracker described in Attachment A belonged to him.



SCOTT BEAGLE

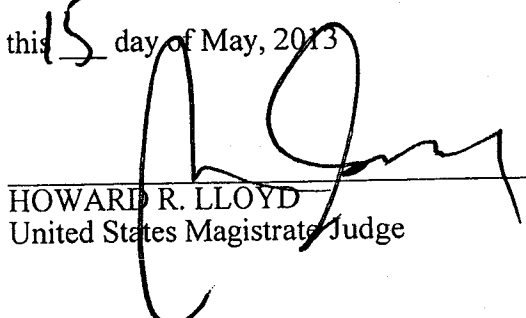
Special Agent

Department of Homeland Security

Immigration and Customs Enforcement

Sworn and subscribed before me

this 15 day of May, 2013



HOWARD R. LLOYD
United States Magistrate Judge

UNITED STATES DISTRICT COURT

for the
District of Columbia

United States of America
v.
John DOE, white male, 45-55 years old,
heavy-set build, balding with wreath of light brown
hair, brown mustache

Defendant(s)

Case: 1:13-mj-361
Assigned To: Magistrate Judge Alan Kay
Assigned Date: 5/10/2013
Description: Complaint and Arrest Warrant

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.
On or about the date(s) of April-May, 2013 in the county of _____ in the
_____ District of Columbia, the defendant(s) violated:

Code Section
18 U.S.C. 2251(a)

Offense Description
Sexual Exploitation of Children

This criminal complaint is based on these facts:
see attached statement of facts

☒ Continued on the attached sheet.

Complainant's signature

Neil O'Callaghan, Special Agent HSI-ICE
Printed name and title

Sworn to before me and signed in my presence.

Date: 05/10/2013

City and state: Washington, DC

Judge's signature

ALAN KAY

UNITED STATES DISTRICT JUDGE

Case: 1:13-mj-361

Assigned To: Magistrate Judge Alan Kay

Assigned Date: 5/10/2013

Description: Complaint and Arrest Warrant

Statement of Facts in Support of Complaint/Arrest Warrant

1. I am a Special Agent with U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement, Homeland Security Investigations (HSI) and am currently assigned to the Cyber Crimes Center, Child Exploitation Investigations Unit (CEIU). I have been employed in federal law enforcement since 1998, and I am responsible for conducting federal and international investigations relating to crimes involving the sexual exploitation of children. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program and have received basic, advanced, and on-the-job training in the investigation of cases involving the sexual exploitation of children. The information set forth in this affidavit is derived from my own investigation, as well as from information obtained from other law enforcement officers. I have not included each and every fact known to me concerning the investigation. I have set forth only those facts necessary to establish probable cause.
2. As a federal agent, I am authorized to investigate violations of United States laws, and to execute warrants issued under the authority of the United States.
3. I am investigating a case of sexual exploitation of a child, specifically the production of child pornography in violation of 18 U.S.C. § 2251(a).
4. On May 3, 2013, HSI received a referral from the Danish National Police related to four videos containing child pornography. The videos had been downloaded from the Internet by law enforcement officers in Denmark. The videos are titled "001", "002", "Ann cums thougha" and "d96ba1a5763a8db4bcac7f3ad0534f9a". The videos appear to have been posted for the first time on the Internet on May 2, 2013. The videos were referred to U.S. law enforcement as Danish Police believed that the video had most likely been produced in the United States. There is no audio present in any of the aforementioned videos.
5. The videos depict an unidentified male ("John DOE") and a prepubescent female, who appears to be approximately 7 - 9 years old, engaged in sexually explicit conduct. The prepubescent female minor lacks post-secondary sexual characteristics including pubic hair and breast development. The videos are inscribed with date stamps that normally correspond to the date the videos were produced, though the accuracy of these stamps depends on the device being used to produce the video to have been set properly. "Ann cums thougha" has a date stamp of April 27, 2013. The remaining three videos have a date stamp of April 14, 2013. The videos are described below:
 - "001" - The video is 1:13 in length and begins by depicting the prepubescent female kneeling on the ground. John DOE is standing in front of the prepubescent female with his pants around his ankles. He is wearing boxer shorts. Visible in the background are musical instrumentation such as guitars, speakers, a keyboard, electronic equipment and a musician stand and stool. John DOE's penis is protruding from his boxer shorts and the prepubescent female places John DOE's penis in her mouth. Throughout the 1:13 video the victim repeatedly places her mouth over John DOE's penis and rubs it with both her right and left hand.

- "002" – The video is 0:52 in length and is filmed in the same location as video "001" referenced in the paragraph above. Again the same prepubescent female victim is kneeling in front of what appears to be the same John DOE suspect. She is wearing the same clothing as in video "001". The victim is also holding a blanket in her right arm. John DOE is wearing what appears to be the same pants and shirt as in video "001". In this video John DOE's penis is protruding through his pants. Throughout the 0:52 video the prepubescent female victim places John DOE's penis in her mouth, holding it in both her right and left hand.
- "d96ba1a5763a8db4bcac7f3ad0534f9a" – The video is 1:05 in length and is filmed in the same location as videos "001" and "002" described in the paragraphs above. The same prepubescent victim and John DOE suspect are depicted. Both are wearing the same clothing as in videos "001" and "002". The video opens with the prepubescent female kneeling on the musician stool. Her exposed anal and vaginal area is facing the suspect and is captured clearly by the camera. The John DOE suspect is sitting in a chair facing the victim's exposed anal and vaginal area and is seen inserting his right index finger into the victim's anus and/or vagina. At the 00:32 mark the video cuts to the suspect kneeling on the floor behind the prepubescent female victim, who is still kneeling on the stool. The John DOE suspect is licking the anal and vaginal area of the victim. At the 00:39 mark of the video the suspect begins wiping the victim's anal and vaginal area with a tissue before continuing to lick her anal and vaginal area and inserting one of his fingers into her anus and/or vagina.
- "Ann cums thougha" – The video is 2:27 in length and filmed in what appears to be the same location as the three videos referenced in the paragraphs above. The video opens with the prepubescent female lying on her back on the floor. The John DOE suspect is also lying on the floor, lying in front of the victim; the victim's legs are positioned over the John DOE suspect's shoulders. His head and back are facing away from the camera and his face is not seen in the video. Throughout the video the suspect appears to be licking the vaginal area of the prepubescent female minor. He appears to be wearing the same pants as in the three videos referenced in the paragraphs above, and although his face is not seen the suspect has the same body shape, proportions and balding hair line and hair color as the suspect in videos "001", "002" and "d96ba1a5763a8db4bcac7f3ad0534f9a".

6. The "John DOE" depicted in this video is described as a Caucasian male, 45 - 55 years in age, with a heavy-set build. He is balding with a wreath of light brown hair and a brown mustache. He appears to have what is commonly referred to as a "beer gut." Four (4) images of "John DOE" are included in Attachment A to this affidavit.

7. In the videos "001", "002" and "d96ba1a5763a8db4bcac7f3ad0534f9a" described above agents have observed what appears to be the bottom half of packaging for a commercially sold food product. Specifically, agents assigned to the HSI Cyber Crimes Center have determined the

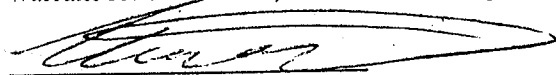
packaging is consistent with a commercially sold bag of Rold Gold "Thins" pretzels. Rold Gold is a Frito-Lay product that is under the Pepsico corporate umbrella. Research conducted of the official Pepsico and Frito-Lay websites revealed that Rold Gold is listed as a product sold in North America, specifically the United States and Canada. Rold Gold is not listed among products sold outside of the United States and Canada. Examination of the Frito-Lay websites for the United States and Canada reveals that Rold Gold pretzels are packaged differently within the United States and Canada. The packaging shown on the Frito-Lay American website matches the packaging observed in the room the videos listed above were produced. The Frito-Lay Canada website displays Rold Gold pretzels with different packaging, including French language descriptions, sold in Canada. On May 6, 2013 the HSI Cyber Crimes Center contacted the HSI office in Vancouver, British Columbia, Canada. An HSI Special Agent assigned to that office observed the Rold Gold pretzel packaging on Rold Gold pretzels sold at a local convenience store chain and grocery store and advised the HSI Cyber Crimes Center that the packaging on the Rold Gold pretzels for sale in Vancouver matched the Frito-Lay Canada website packaging example. That is to say, the packaging observed by the HSI agent in Vancouver did not match the packaging seen in the videos described above. Based on this analysis it is my belief that the Rold Gold pretzel bag observed in the videos was exclusively distributed within the United States.

8. This Court has jurisdiction over the offense under investigation pursuant to 18 U.S.C. § 3238, which provides, in relevant part, that jurisdiction for "[t]he trial of all offenses begun or committed . . . out of the jurisdiction of any particular State or district, shall be in the district in which the offender . . . is arrested or is first brought; but if such offender . . . [is] not so arrested or brought into any district, an indictment or information may be filed in the district of the last known residence of the offender . . . , or if no such residence is known the indictment or information may be filed in the District of Columbia." In this case, the child pornography video described above was transported in foreign commerce, in violation of 18 U.S.C. 2251(a); therefore, the offense was "committed outside the jurisdiction of any particular State or district." In addition, the identity of the defendant is not known and, therefore, no last residence of the offender is known. As such, this Court has jurisdiction over the offense under investigation.


CONCLUSION

9. Based on the information set forth in this affidavit, I submit that there is probable cause to believe that John DOE has produced, possessed and distributed child pornography, all in violation of Title 18, United States Code (U.S.C.), § 2251(a).

10. In consideration of the foregoing, I respectfully request that this court issue an arrest warrant for John DOE, described and depicted in Attachment A.


Neil J. O'Callaghan, Special Agent
US Immigration and Customs Enforcement

Subscribed and sworn to before me this 10th day of May, 2013.


United States Magistrate Judge

ALAN KAY
U.S. MAGISTRATE JUDGE

Attachment A

